NATIONS UNIES **E**

Conseil Économique et Social

Distr.
GÉNÉRALE

CES/AC.71/2001/17 (SUM)
5 décembre 2000

FRANÇAIS
Original : ANGLAIS

COMMISSION DE STATISTIQUE et COMMISSION ÉCONOMIQUE POUR L'EUROPE

COMMISSION DES COMMUNAUTÉS EUROPÉENNES (EUROSTAT)

CONFÉRENCE DES STATISTICIENS EUROPÉENS

Réunion commune CEE/Eurostat sur la gestion de la technologie de l'information en statistique
(Genève, Suisse, 14-16 février 2001)

Point ii) : Défis et possibilités pour les services de statistique travaillant en réseau

LES PROBLÈMES DE SÉCURITÉ POSÉS PAR LE TRANSFERT DE DONNÉES VIA DES RÉSEAUX ET LES SOLUTIONS MISES EN ŒUVRE AU BUREAU CENTRAL DE STATISTIQUE POLONAIS (BCS)

Document présenté par le Bureau central de statistique polonais [1]

DOCUMENT SOUMIS SPONTANÉMENT

RÉSUMÉ

1. La sécurité des informations statistiques collectées, traitées et diffusées est prise très au sérieux par tous ceux qui travaillent au Bureau de statistique. Indéniablement, il n'est pas possible de mettre en place un système dont la sécurité soit parfaite à tous égards. Dans la pratique, nous estimons qu'un certain risque doit être accepté car, si les systèmes de sécurité se perfectionnent sans cesse, il en va de même des techniques de piratage. En conséquence, une protection efficace des informations confidentielles passe par la détection des points faibles éventuels, qui risquent de porter atteinte à la confidentialité, à l'intégrité ou à la disponibilité de ces informations. Dans chaque domaine où il existe des risques, il faut recenser les moyens plausibles de déjouer le dispositif de sécurité et mettre au point des contre-mesures. À cet égard, il peut être utile de faire appel aux services d'entreprises spécialisées dans les systèmes de sécurité des données.

2. La politique de sécurité porte sur toutes les tâches des responsables de la gestion et de l'administration, du personnel technique, des utilisateurs et de tous les autres membres de l'organisme

[1] Préparé par Halina Agnieszka Stegawska

considéré, en vue de maintenir le niveau de sécurité nécessaire du système d'informations statistiques. Ce niveau de sécurité est déterminé par le nombre de dispositifs de sécurité utilisés. Ceux-ci ont trait à l'accès aux ressources (matériel, logiciels, documents, données brutes), à la confidentialité de données, à l'authentification et à l'intégrité des données.

3. Les risques d'échec du dispositif de sécurité protégeant les données dans les réseaux informatiques se répartissent en trois catégories principales :

- Mise en échec intentionnelle du dispositif de sécurité : vol d'une clef de codage ou intrusion dans un réseau;

- Accès non autorisé aux données par une personne qui se connecte en utilisant un mot de passe volé ou deviné;

- Impossibilité d'obtenir des services, lorsqu'en raison d'un échec du système de sécurité, des utilisateurs ne peuvent obtenir une partie ou la totalité des services offerts par un réseau ou un serveur.

4. Les principales techniques qui sont déjà utilisées ou qu'il est prévu d'utiliser pour assurer la sécurité des réseaux sont l'identification (au moyen d'un mot de passe), l'authentification (vérification de l'identité de l'utilisateur), l'autorisation et le contrôle d'accès (attribution de droits d'accès à un utilisateur), la protection de la confidentialité des informations, l'intégrité des données (mesures empêchant l'altération d'un document lors de son transfert) et les signatures numériques.

5. D'autre part, il faut assurer la sécurité de l'accès à l'Internet ainsi que de l'accès au réseau étendu du Bureau central de statistique (BCS) via l'Internet. Toutes les ressources de traitement de données de l'intranet du BCS sont protégées par un coupe-feu et ne sont donc pas accessibles depuis l'extérieur. Seuls des serveurs Web diffusant des bases de données publiques à l'extérieur du coupe-feu sont accessibles via l'Internet. Les personnes qui travaillent dans les bureaux régionaux de statistique et qui utilisent le réseau local du BCS doivent passer par le coupe-feu central pour avoir accès à l'Internet. Une authentification de l'utilisateur est nécessaire pour la connexion à l'Internet et il faut disposer d'une autorisation pour des services tels que le courrier électronique, le Web, Telnet et FTP. Le coupe-feu est complété par deux routeurs supplémentaires, ce qui rend plus difficile encore toute tentative d'intrusion dans le système.

6. Il faut constamment mettre à niveau le système de sécurité des données, en utilisant des techniques nouvelles qui renforcent la sécurité. En conséquence, le BCS s'emploie à apporter des améliorations dans les domaines suivants :

- La détermination des points faibles du coupe-feu actuellement utilisé, son amélioration et son remplacement éventuel;

- L'adoption du système d'exploitation Windows 2000 Server et Windows 2000 pour les PC;

- Le remplacement d'une partie du matériel connecté aux réseaux locaux et au réseau global du BCS par du matériel offrant une plus grande sécurité, par Switch L3 et de nouvelles générations de routeurs, par exemple;

- Le codage des données se trouvant sur le serveur et le réseau étendu;

- La mise à jour régulière du Règlement d'utilisation des réseaux informatiques et l'amélioration de son observation.